**DOS Attack: SYN Flooding**

Each team will be assigned a type of denial of service (DoS) attack. The teammates will be responsible for the following parts of the project.

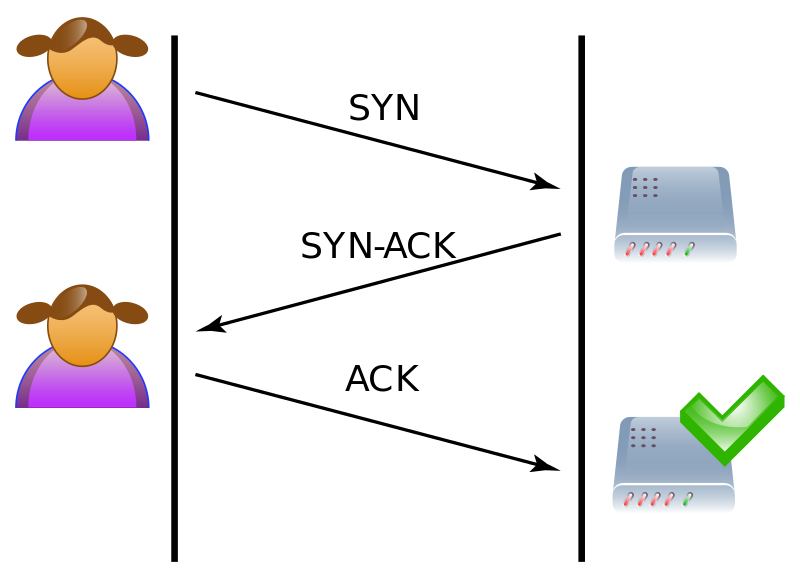
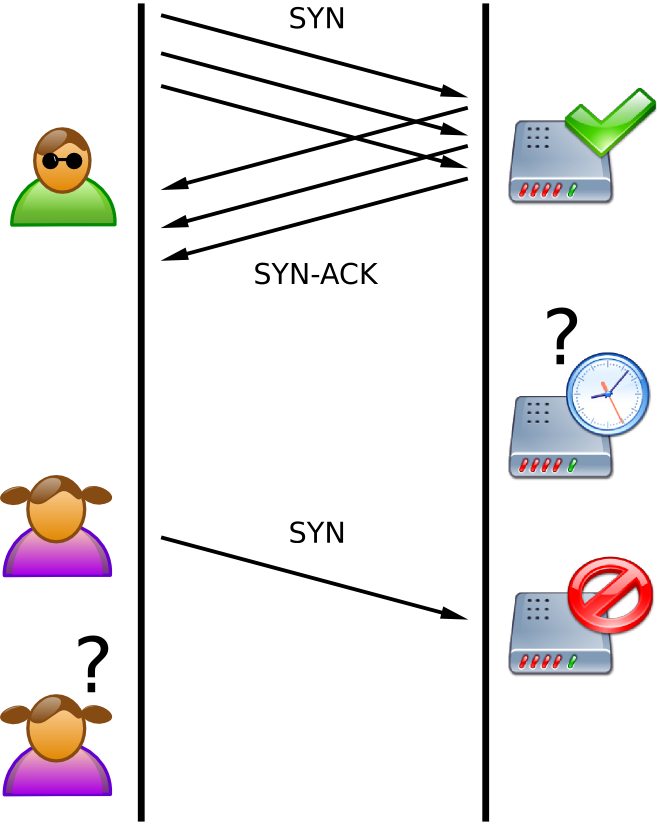
Teammate 1 - Describe the history of the attack. Who has used it? When and where? Who did they attack? When was it discovered? What is the objective of the attack? Why is it difficult to detect or defend against?

Teammate 2 - Describe the mechanics of the attack. On which OSI layer does it operate? Which protocol/packets does it involve? What does it do to the protocol/packets? How does it achieve its goal? How long does it take to implement? Does it require/use bots, download of malware to attacked computer, etc.?

Teammate 3 - Describe how Wireshark can be used to detect the attack. Show screen shots of where you would look to find evidence of the attack. Show the contents of the packets you need to examine. Demonstrate with screen shots that Wireshark can do these things.) Describe if Wireshark can only detect the attack during the attack, or can only detect the attack after the attack, or both. Explain why.

Note: You do not have to demonstrate the attack itself, just show how Wireshark could be used detect it

**What is SYN Flooding? (Andoni)-**

* **2-3.5 columns**
* An overview of your group's denial of service attack type.
  + Transmission Control Protocol, or TCP, typically connects to a server by sending a connection request with a synchronize, or SYN, message. After the server acknowledges the request, it sends back a sychronize-acknowledge, or SYN-ACK, message. Finally, an acknowledge, or ACK, message is sent back to acknowledge, finally establishing a connection. This is what is known as a three-way handshake. An SYN flood is a denial of service attack that sends thousands of spoofed requests to connect that are meant to overwhelm the server. As the server tries to send back the numerous amount of SYN-ACK messages, because there is nothing there to receive them, the server could eventually even crash.
* Describe the history of the attack.
  + One of the most famous SYN flood attacks, and one of the first DDoS attacks in history, is the Panix incident in September of 1996. [2] Panix is New York’s oldest commercial Internet provider.
  + While we do not know how specifically long it took for the attack to be identified, a DDoS attack on this scale can be noticed quite quickly, especially if the intent is to cause mass disruption. The perpetrating hacker had not seemed to be identified, or at the very least, not publicly disclosed. While not officially confirmed, it is speculated that the attack was regarding the recently installed system for email blocking at the time. [1]
  + This attack caused Panix to be shut down for a week, affecting thousands of users and companies to Internet access. [3]
  + Another well-known attack using SYN floods is the WikiLeaks attack from 2010. As WikiLeaks was releasing leaked information regarding US embassy cables, they were hit with a DDoS attack by a group of hacker activists, or hacktivists, that were trying to take them off the Internet. One of their main methods of attack was using SYN floods to slow down the leaks. [4]
  + There are multiple other attacks involving SYN floods, such as the Yahoo! one in 2000, the Boston Bomb Scare in 2007, and the ransomware attack on the University of California, San Francisco a few years ago in 2020.
* Why is it difficult to detect or defend against this type of attack?
  + Although there are many reasons that defending against a SYN flood attack can be difficult, some major issues include the large volume of traffic, how fast the attack can occur, and the spoofed IP addresses. Due to the amount of SYN packets that occur, a high volume of traffic is created, causing the network to be overwhelmed. Hackers are able to execute this type of attack quickly, making it harder for any protection in place to respond in a timely manner. With spoofed IP addresses being used, it makes finding the origin of the attack and how to block traffic efficiently difficult.
  + Some counteractions may include limiting the rate of SYN packets and implementing instructions prevention systems, or IPSs, and firewalls. By limiting the rate of SYN packets, one can prevent an excessive amount of connection requests from a single source. Installing IPSs and firewalls can also help prevent a SYN flood from occurring, by helping filter traffic and being to detect things, such as anomalies, such as the sudden appearance of requests.
* [](https://en.wikipedia.org/wiki/SYN_flood)
* **Fig. 1. A typical three-way handshake connection:** A demonstration of how a user can connect to a server. First, a SYN message is sent. After the server acknowledges the requests, it returns a SYN-ACK message. Finally, the user responds with an ACK message, establishing a connection.
* [](https://en.wikipedia.org/wiki/SYN_flood)
* **Fig. 2. How a SYN flood attack typically looks like:** A demonstration of how a SYN flood attack works. First, after the attacker sends a numerous amount of packets, the server tries to respond with several ACK messages. Because the server does not receive the corresponding ACK messages. A typical user will try to establish a connection like normal, but because it is consuming resources to deal with the SYN flood, it is unable to.

References:

* <https://archive.nytimes.com/www.nytimes.com/library/cyber/week/0914panix.html> [1]
* <https://www.proquest.com/docview/2625916480?pq-origsite=primo&parentSessionId=yPmO8f18hDOpgyqz75Rtlorw%2BmxkRqGdKf%2B3BDKOuSY%3D> [2]
* <https://go-gale-com.lp.hscl.ufl.edu/ps/retrieve.do?tabID=T003&resultListType=RESULT_LIST&searchResultsType=SingleTab&retrievalId=520fbf50-331f-4ca3-8fcd-16a615a7f925&hitCount=1&searchType=AdvancedSearchForm&currentPosition=1&docId=GALE%7CA18706982&docType=Column&sort=RELEVANCE&contentSegment=ZONE-MOD1&prodId=AONE&pageNum=1&contentSet=GALE%7CA18706982&searchId=R1&userGroupName=gain40375&inPS=true> [3]
* <https://www.theguardian.com/media/2010/dec/07/wikileaks-under-attack-definitive-timeline> [4]
* <https://academic.oup.com/comjnl/article/62/4/518/5183521?login=true>

**Mechanics of SYN Flooding (Emmanuel)**

1. Mechanics [1]
2. A SYN flooding attack works by repeatedly sending SYN packets, synchronize or initial connection request packets, to a server which will overwhelm the ports on a machine and cause it to be extremely slow or not function at all.
3. This attack works by exploiting the handshake process of a TCP connection. The way the handshake process in a TCP connection is as follows
   1. First a client must send a SYN packet to the server
   2. Next, the server responds to that packet with an SYN/ACK packet to establish communication
   3. After the client receives the ACK from the server, the client will respond with an ACK and now a TCP connection is established between the client and the server

B. OSI Layer

1. A SYN Flooding attack works on OSI Layer 4. Layer 4 of the OSI model is the transport layer. [2]
   1. The transport layer is responsible for network traffic between a client and a server and ensures complete data transfers.
   2. To ensure complete and correct data transfers, a TCP connection uses a three-way handshake process.
   3. This handshake process is exploited in a SYN flooding attack

C. Involved Packets

1. The packet used for the attack is a SYN packet. SYN is synchronize and is a TCP packet sent to another client or server which requests to establish a connection between them [3]
2. An ACK package is sent in response after a SYN packet is received. ACK is short for acknowledgment and simply indicates that the data has been received successfully. [4]
3. If the original client that sent the SYN packet receives an ACK from the server, an ACK is sent by the client

D. What it does to the packets/How does the attack work

\*talk about the different types of SYN packet attacks maybe\*

1. The attacker will likely modify the SYN packet by sending it with a spoofed IP. What this does is that the SYN/ACK packet sent by the server will be sent to a random IP. The server will then be waiting for an ACK packet from an IP that it never established a connection with.
2. Also, the attacker will never send the ACK packet either. The server is now waiting for an ACK packet that will never arrive but it keeps its ports open to it, wasting resources
3. The attacker will repeatedly send SYN packets as this will clog up the ports of the server making it so that the server is continually waiting for ACK packets from the client and not doing much else. This makes it so the server will not function as normal [1]

E. How long does it take to implement?

1. This attack does not take much time to implement. A basic version of this attack can be done using the hping command in the command line and some settings on it to exploit the TCP three way handshake [5]. (Unspoofed version) The attack can then be ran for as long as the attacker wants and it was fairly easy to implement.

F. Does it require/use bots, download of malware to attacked computer

An effective attack will likely require a botnet to fully deny internet service to the victim. This is because a direct SYN attack is easy to defend against as the victim can simply block the attacker's IP. If the attacker uses a botnet, blocking the individual IPs of each bot becomes much more difficult and it also becomes much harder to trace back to the attacker.

**References:**

<https://www.cloudflare.com/learning/ddos/syn-flood-ddos-attack/> [1]

<https://www.a10networks.com/glossary/what-is-layer-4-of-the-osi-model/> [2]

<https://www.computerhope.com/jargon/s/syn.htm> [3]

<https://www.techtarget.com/searchnetworking/definition/ACK> [4]

<https://vlab.amrita.edu/?sub=7&brch=199&sim=365&cnt=2> [5]

**How can wireshark be used? (Gary)-**

Teammate 3 - Describe how Wireshark can be used to detect the attack. Show screen shots of where you would look to find evidence of the attack. Show the contents of the packets you need to examine. Demonstrate with screen shots that Wireshark can do these things.) Describe if Wireshark can only detect the attack during the attack, or can only detect the attack after the attack, or both. Explain why.

Note: You do not have to demonstrate the attack itself, just show how Wireshark could be used detect it

How Can Wireshark Be Used to Detect the Attack? ( 2-3.5 columns)

Describe how Wireshark can be used to detect your group's assigned DoS attack. Show screen shots of where you would look to find evidence of the attack. (The evidence may not be in the same place where the attack occurs.)

Use Wireshark screen shots of actual traffic to show the contents of the packets you need to examine to detect the attack. You do not have to demonstrate the attack itself, just show where in the packets and/or packet contents the a Wireshark user would be able to find evidence of the attack.

Describe if Wireshark can only detect the attack while the attack is happening, or if it can detect the attack only after the attack happened, or both. Explain why.

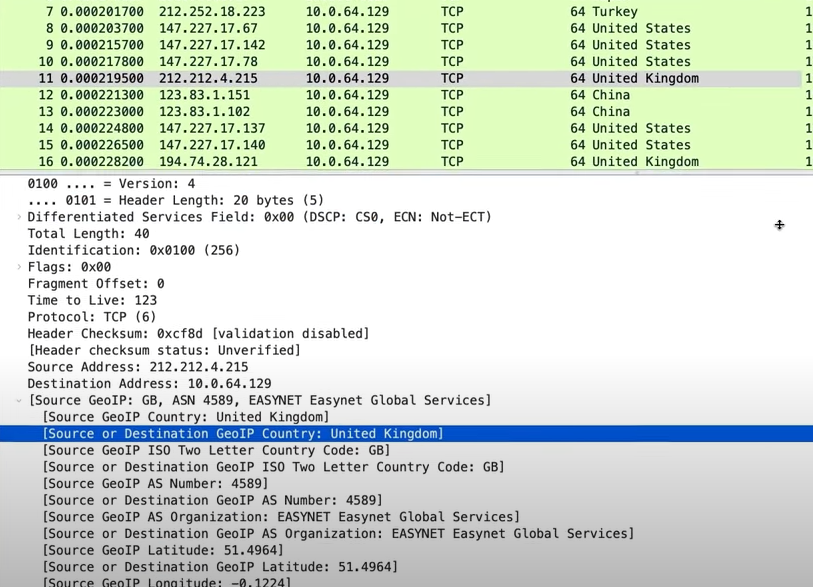
References  
<https://subscription.packtpub.com/book/cloud-and-networking/9781785887819/7/ch07lvl1sec43/the-dos-attack>

[Using Wireshark to Detect a SYN Flood Denial of Service Attack](https://www.youtube.com/watch?v=VBUxA_95KoY)

[Is this an attack? Wireshark Packet analysis // SYN Attack](https://www.youtube.com/watch?v=8mLt3QPZJtY)

Using wireshark to detect and mitigate a SYN flood attack

1. Detecting using wireshark  
   If you notice your network starting to slow down or shut off entirely, you might be experiencing an attack. Using a program such as wireshark in order to recognize an attack,  
   If there's a large number of incoming SYN packets that were not followed by corresponding ACK packets. Attempting to initiate connections without completing the handshake.

One way to identify an attack versus normal tcp usage is to look at the \_\_\_\_ addresses of the TCP packets. In wireshark, it is possible to import databases of known ip addresses and automatically label them based on location. One such database is GeoIP. Typically a business would get traffic from a certain demographic area so we can make assumptions that packets from countries we wouldn't normally do business with, we can mark them as suspicious.  
  
In wireshark its possible to filter and mark packets using the labels they are given. In order to visualize sketchy packets, we might want to change the color of the display in wire shark and then see how many of the incoming tcp packets are from weird locations.   
  
Another factor to consider is

1. Timing between the packets  
   The timing between the packets will be small, between \_\_\_\_ seconds. This is all variable depending on the
2. Normal syn handshake vs attack
3. Going back to check afterward